Cybercriminals Have Passed Law Enforcement By Let's Catch Back Up!

by

Thomas Chaplin
Citrus Heights Police Department

May, 2009

Command College Class 44

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

Cybercriminals Have Passed Law Enforcement By Let's Catch Back Up!

Now even the crooks are telecommuting. Criminals no longer have to leave the luxury of their own homes to commit criminal activity. Sitting at their very own residence – in the comfort of their pajama bottoms and slippers – they can reach into unsuspecting victims' homes and steal identification and money from their unwitting victims, whether they are young professionals or your grandparents living on a fixed income. Sound far-fetched? It happens every day.

New and ever evolving methodology employed by criminals using computers and the Internet to commit crime improves on a daily basis. Law enforcement has yet to catch up to these cybercriminals. In many law enforcement agencies, investigators do not have the training or technical computer acumen, nor do the departments have the budgets to investigate these cybercrimes. (Schwartau, 2000) Echoing this sentiment is Alan Youngs, a retired 33-year veteran and former division chief of the Lakewood, Colorado police department. Youngs, a past-president of Police Futurist International and a member of the Futures Working Group, wrote in 2005 that "the complexity of criminal investigations is evolving at a pace that matches the changes in technology and society as a whole." (Youngs, 2005) This has evolved to a situation where some police agencies even intentionally avoid computer related crimes because they are complex, demanding, and time-consuming (Schmalleger, 2006) There is, though, another way.

Law enforcement could deliver a higher level of customer service and respond to computer crimes more effectively by hiring computer technology graduates right off the street and assigning them to investigate technology based crimes. Hiring recent graduates of collegiate information technology programs as civilian investigators could

enable policing to begin catching up to technology based crimes. The time is right for this opportunity; the question should not be whether to, but how to implement such change.

Changes in Technology = Changes in Crime

In North America alone, estimates reveal there were more than 246 million Internet users in 2008; an increase of 128% since 2000. This represents a usage rate in the US of about 73% of the total population. (U.S. Census Bureau, 2009) The number of estimated users worldwide in 2008 was over 1.5 billion. This represents an estimated growth of over 336% since the year 2000. (http://www.internetworldstats.com, 2008) Along with the myriad of legitimate uses and enhancements in interconnectivity, the use of the Internet to assist or commit crime is exploding at the same rate.

Crimes perpetrated via the Internet have negatively impacted a growing segment of society. Studies show that "11% of senior citizens, 65 and over are likely victims of Internet identity theft." (AARP Consumer Protection Team, 2009) The Internet site InsideIDTheft.info notes that "Many identity crimes, crimes of deception and financial crimes are traditionally aimed at our senior population as criminals believe seniors may be more susceptible to crimes of deception and the amount of money that can be stolen from a senior may exceed that of other segments of the population." (Inside ID Theft, 2009) This is not to say that computer related criminal activity is solely aimed at seniors; rather bankers, celebrities, company heads, children, and even dead people are susceptible to cybercrime. (Hammond, 2003)

Advances in technology associated with computers and the Internet have led to changes in criminal methodology. It now does not take a great level of sophistication to cause a lot of harm to people. Simple access to a Google search key reveals a wealth of "how to" information on the Internet. By inputting "how to steal identity on the Internet" would-be criminals can quickly learn tricks of the nefarious high technology crime trade. Sadly, the information readily available can lead to easy mining of the Internet for "nuggets of personal information" which can lead directly to access to personal identities and online bank accounts. (Thompson 2008)

Identity theft is only one of the ways in which criminals are utilizing the Internet to commit crimes. According to a 2007 survey conducted by the Internet Crime Complaint Center, the most prevalent complaint categories in California alone in 2007 were: 1) Auction Fraud 2) Non Delivery of Merchandise /Payment 3) Confidence Fraud 4) Credit Card Fraud 5) Computer Fraud 6) Check Fraud 7) Identity Theft 8) Financial Institutions Fraud 9) Nigerian Letter Fraud, and 10) Threats. The National White Collar Crime Center base their annual reports on complaints received and referred by the Internet Crime Complaint Center (IC3) to law enforcement or regulatory agencies for appropriate investigative action. The 2007 report featured the following chart depicting the number of complaints reported between 2000 and 2007. As one can see, the criminal "con man" of the future is on-line; he or she is also quite busy.

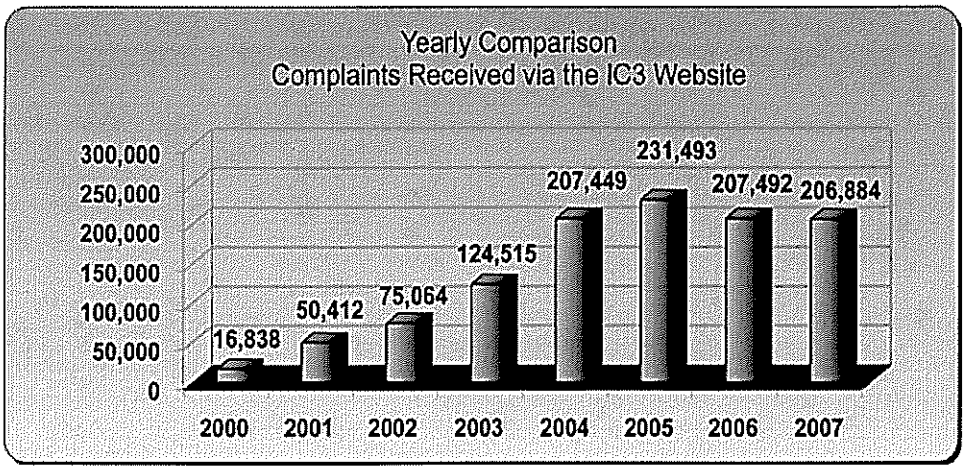

Chart used with permission from the IC3

Cyberspace and the New Confidence Man

In 1849 the term "Confidence Man" was coined to describe a breed of criminal that was "suited to the highly mobile, anonymous social milieu of nineteenth-century America." (Cole, 2001) This con man could abuse the trust of others and adopt a new identity. Often the con man would reappear in a new town with the assumed identity and commit crimes of fraud. What made the con man so dangerous was the "ability to counterfeit not only bank notes or documents, but entire identities." (Hammond, 2003)-

The requirements that led to the successful activity of the con man are much easier to attain today. Whereas over a century ago a con man had to rely on moving from city to city to stay anonymous, mobility is instantly available to the modern con man. Anonymity is easily attained; travel takes place in cyberspace as the con man sits in the comfort of his or her home (Abbate, 2000). Cyberspace provides the opportunity for users to create and explore imaginary environments, establish new forms of communities, and to "experiment with different identities." (Abbate, 2000) Unfortunately, cyberspace also opens up a vista of potential new victims to the criminally inclined.

With the freedom to move about anonymously, today's con man, or cybercriminal has a variety of victims to take advantage of, as well as a variety of means and methods. Many of today's technology based crimes are simply updated versions of age-old scams with a new and improved methodology. (Abagnale, 2000) After years as a prolific con man, Mr. Frank Abagnale was captured and sentenced to prison. During his heyday, he engaged in criminal activity in which he practiced law without a license; posed as a college professor; and cashed over 2.5 million dollars in forged checks. He had several different identities, and conducted most of his illicit activity before he turned 21-years-old. (Abagnale, 2000)

Abagnale's FBI pursuers used good, old-fashioned police work and "shoe leather" to track him down. With Abagnale's progeny now on-line, what means can we use to bring them to justice?

Law Enforcement Response to Cybercrime...So Far

Law enforcement has been slow to keep pace with these advances in technology. One of the reasons for the slow response is the focus on reducing more violent crimes. (Goodman, 1997) Gang members, drug dealers, and other more obvious examples of neighborhood crime issues are the more common source of police related calls for services. In fact, there are far more cybercrimes to investigate than available resources to conduct the investigations. (California State and Consumer Services, 2005) This issue is not limited to the United States; British police are also facing the same problem. One senior official with London Metropolitan Police stated "the scale is such that the police service would fall over if it tried to investigate every case. I would hate any member of

the public to feel that they can't report a crime, but people need to understand that each individual e-crime can't be investigated." (Johnson, 2007)

In addition to the lack of resources, law enforcement has difficulty keeping up due to the lack of knowledge and training in the field of computer technology. With regard to identity theft, one recent report noted, "Not all police agencies in the state are equipped to take the initial police report – either because they don't have the personnel or because they don't recognize the crime." (California State and Consumer Services, page 9, 2005) Peter Sacco, an instructor at Canada's McMasters Centre for Continuing Education, writes, "Most perpetrators are always one step ahead, technologically, than the police." He added that police officers, who lack the training and experience, could be up against "really ingenious, computer-skilled college and university graduates paid loads of money." (Powell, 2007) Sergeant Ed Dadisho of the Los Angeles Police Department states firmly that law enforcement leaders recognize the need to keep up with cybercrime by training officers and investigators in reporting, investigating, and preparing cases for court in such matters as identity theft. (Dadisho, 2005)

So if technology based criminal activity is easy to commit and difficult to investigate, what is the best way to stop it from occurring? Historically, the threat of jail has served as the deterrent. Currently, there is little chance that the perpetrators of these crimes via the World Wide Web will be detected, apprehended, and prosecuted. The current means of assigning computer crimes to veteran investigators, or even training cops to investigate web-based crime, falls short of the need to "keep pace" with this emerging crime. There is, though, another way.

Maybe We Need a Different Approach

Traditionally in the field of law enforcement, new recruits are assigned to work patrol, or custody assignments for several years before they are allowed to compete in the selection process for investigative assignments. (Legal-Criminal-Justice-Schools, 2009) This experience dealing with the "criminal element" can be very beneficial to law enforcement professionals in investigative assignments. (Hudock, 2009) For certain specialties, such as homicide, robbery, fraud, and child abuse, it can take several years to attain the necessary training to establish a decent competency in the specialty area.

With the requirements of training to competently investigate these crimes, it can take several years for a peace officer to acquire the acumen necessary for success. According to Sgt. Ronald Levine of the Foothill-DeAnza College District Police Department in Los Altos Hills, California, "There are some basic skill sets you will need before you can start chasing evildoers on the Internet. The investigator needs a thorough understanding of the involved technology." Levine added, "If an officer or deputy doesn't have computer skills, they're going to have to come up to speed and understand how the technology works before he or she can become an effective investigator." (Griffith, , 2003) Realistically, a computer crimes investigator will have a profusion of cases to work as "new technologies give shape to new forms of crimes and methods for their commission." (Schmalleger, 2006) The text Criminology Today concurs, noting "The very nature of contemporary society dictates that crimes exploiting high technology will always be with us." (Schmalleger, 2006)

A better approach to resolve the competency gap in police high-tech investigations – and possibly to make modern day policing desirable to some - would be

to hire recently graduated computer technology majors into technology based investigative assignments.

Hmm, Maybe We Should Hire for Need

Hiring civilian specialists would provide immediate support to technology-based criminal activity. These civilian investigators would be able to invest their time and efforts into the cases that are currently falling through the cracks due to staffing shortages and the lack of the technical acumen to properly investigate technology based offenses. According to John Palfrey, Professor of Law and Vice Dean at Harvard law School, and Urs Gasser, faculty fellow at the Berkman Center for Internet & Society at Harvard law School, the generation entering the workforce feature individuals known as "Digital Natives," those who grew up with networked digital technologies and the skills to use them proficiently. (Palfrey & Gasser, 2008) They are as comfortable living online as they are offline. They intuitively understand how to function in a connected world. (Palfrey & Gasser, 2008) There are highly educated individuals coming out of college with a greater level of technical computer related than current detectives have. Hiring these individuals – at a cost savings to law enforcement agencies - could immediately impact the problems associated with technology based crimes.

By utilizing this approach, law enforcement leaders could respond to an area of need and enhance customer service to their respective communities. Beyond their specific value as investigators, they could also provide training for others to enhance the overall agency expertise. Learning from computer technology specialists is already benefitting the Federal Bureau of Investigation. Purdue University's Cyber Forensics Lab

partners with the FBI's Indianapolis Office for consultation and training (Purdue University, 2008).

The retention of civilians to perform traditional law enforcement actions is not a new concept. In San Francisco, the police department has been involved in civilianizing many positions in order to increase overall effectiveness, and to get sworn officers out of the office and onto the streets. According to the San Francisco Chronicle, "The impetus isn't just financial: Studies have shown that adding civilians to a police force can help departments respond better to community needs and react more quickly to changes in technology." (Lagos, 2008) There are substantial salary savings that come with using civilian staff, which is a potential secondary benefit for law enforcement leaders. In an in-depth study of the Dallas Police Department's operations, the researchers opined that the primary reason civilians should be hired to perform jobs that don't require a sworn officer is because civilian personnel are much less expensive. (Griffiths & al., 2006)

There are a number of agencies seeking ways to incorporate civilian personnel to augment their police services. In East Mesa, Arizona, a pilot program will begin the summer of 2009, in which civilian crime "specialists will respond to lower-level crimes and dedicate themselves to taking reports without interruption, or hopefully, long delays." The intention of the pilot program was to free sworn personnel for more serious crimes that could jeopardize someone's safety. (Sakal, 2009) Civilian personnel also assist the processing of evidence. Chief Ronald Davis, of the East Palo Alto Police Department in California, believe that departments must learn how to use civilians to provide police services at a time when agencies are dealing with the challenge of shrinking budgets. (Bune, 2009) Civilians working in law enforcement are not a novel concept; however,

targeting a college graduate for a specialist assignment investigating cybercrimes just might be.

The potential for negative consequences exist anytime there is discussion of new positions or a redirection of existing positions in law enforcement. Depending upon current budget conditions at any involved agency, the possibility of replacing a sworn peace officer position with a civilian position could cause consternation with existing law enforcement staff. One study spearheaded by the Vancouver Police Department in Canada, with input from Canadian and American law enforcement agencies, found that movements to add civilian personnel in lieu of sworn officers has been met with concern by senior police management, unions, and associations fearing that civilianization would lead to less job security and promotional opportunities. (Griffiths et al., 2006) Other questions would need to be addressed as well. For example, would victims of cybercrime be amenable to having their case investigated by civilian law enforcement personnel?

An expert panel was convened to discuss the topic of hiring recently graduated cybercrime investigators. These experts included law enforcement investigators from the municipal and state level, small business owners, and a retired police sergeant. The retired police sergeant, Darrell Freeman, works for Bank of America Corporate Security and is a Vice President Security Manager responsible for Northern California. He is also president of the Sacramento Citizens' Crime Alert Reward Program. Freeman opined that law enforcement needs to take advantage of the highly educated and motivated youth coming out of college. He said, "There is a lot of great talent coming out of the world of academia that could help law enforcement quickly. These kids might not want to push patrol cars, but that does not mean they can't contribute to stopping crime."

What Would This Look Like

The creation of a civilian cybercrime investigator positions would necessitate the creation of a proper training program. Once a cybercrime investigator is hired, a training program would be implemented to ensure that the individual is properly acclimated to the assignment and the involved agency. Traditionally, sworn officers/investigators are required to attend and successfully complete a POST basic recruit academy. The best fit for a newly hired civilian investigator would be a community services officer training academy (or similar orientation course) for proper exposure to police work. Per the POST website, the community services officer academy covers "professionalism and ethics, report writing, property crimes, crime scene management, accident investigation, vehicle operations, missing persons, and tactical communications." (California Commission on Peace Officer Standards and Training, 2009).

Once the civilian investigator successfully completes the academy, a training program would be established with current field training officers and detectives. This in-house training program would be conducted in an effort to teach the civilian investigator the involved law enforcement agency's internal reporting procedures. The detective training would be focused on the investigation of criminal cases and the filing of completed cases with the local district attorney's office. Once the training program is complete – and the investigative sergeant believes the civilian investigator is ready to conduct criminal cases – criminal investigations involving technology will be assigned. Although this approach is novel, industry experts see it as one with merit.

Future Perspective of Computer Technology Investigators

Greg Cowart has over forty years of experience as a peace officer in the State of California. He has served as the Police Chief in the cities of Gilroy, Roseville and Millbrae and was the Director, Division of Law Enforcement, California Department of Justice for eight years. Cowart steadfastly believes that the local law enforcement agencies need to adopt a model similar to that of the military and Federal law enforcement agencies, which have been "recruiting the best and brightest linguists and technical minds directly from institutes of higher learning for years." He added, "Many of our children and grandchildren will grow up to be patriotic, hard-working and reliable; and they will have cyber-skills we have only dreamed of. Perhaps they have no desire to carry a gun or handcuffs, but they possess skills that will identify hi-tech criminals and lead to their apprehension and prosecution." He believes the time is right for local law enforcement to begin recruiting young men and women right out of college or specialized military units and into cyber-crime units.

There are highly educated individuals coming out of college with a greater level of technical computer knowledge related than many current technology based crime investigators. Hiring these individuals – at a cost savings to law enforcement agencies - could immediately impact the some of the problems associated with investigating technology based crimes. Waiting for a police officer to get trained in the area of high technology crimes is too lengthy a process. Every day wasted is a new opportunity for the criminals, and a potential for victimization of an unsuspecting community member.

Conclusion

By hiring civilian investigator computer specialists, many more cases could be investigated. This will help the victims of these crimes have closure. It is important that we in law enforcement always remember the Law Enforcement Code of Ethics, which states in part, "With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately..." (California Commission on Peace Officer Standards and Training, 2007) The victims of these crimes deserve our best efforts. There is an emotional impact to the victims of identity theft, with some experiencing a form of short-term post-traumatic stress disorder. (Hammond, 2003) Law enforcement owes it to the communities they serve to try and get in front of cybercrime, rather than letting it continue to pass us by.

Works Cited

AARP Consumer Protection Team. (2009, March 7). *Senior Internet Identity Theft.* Retrieved March 7, 2009, from BroadbandInfo.com: http://www.broadbandinfo.com/high-speed-internet/seniors/identity-theft.html

Abagnale, F. W. (2000). *Catch Me If You Can: The Amazing True Story of the Youngest and most Daring Con Man in the History of Fun and Profit* . New York: Broadway Books.

Abbate, J. (2000). Inventing the Internet. In J. Abbate, *Inventing the Internet.* Cambridge: The MIT Press.

Bune, K. L. (2009, Febrauary 2). *Civilian Roles In Policing: Increasing numbers are wave of future*. Retrieved March 10, 2009, from Officer.Com: http://www.officer.com/web/online/Leadership/Civilian-Roles-In-Policing/16$45206

Bureau of Labor Statistics. (n.d.). *Occupational Outlook Handbook, 2008-09 Edition, Police and Detectives*. Retrieved March 8, 2009, from Bureau of Labor Statistics, U.S. Department of Labor: http://www.bls.gov/oco/ocos160.htm

California Commission on Peace Officer Standards and Training. (2007, October 17). *POST Administrative Manual* . Retrieved March 8, 2009, from California Commission on Peace Officer Standards and Training, Publications: http://www.post.ca.gov/Publications/PAM/

California Commission on Peace Officer Standards and Training. (2009). *POST Course Catalog*. Retrieved March 17, 2009, from California Commission on Peace Officer Standards and Training, Publications, Course Catalog: http://www.post.ca.gov/Publications/Course_Catalog/2287.asp

California State and Consumer Services. (2005). *LOCKING UP THE EVIL TWIN: A SUMMIT ON IDENTITY THEFT SOLUTIONS.* Sacramento: California State and Consumer Services Agency.

Cole, S. A. (2001). Suspect Identities: A History of Fingerprinting and Criminal Identification. In S. A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (p. 21). Cambridge: Harvard University Press.

Dadisho, E. (2005, January). Identity Theft and the Police Response: The Problem. *The Police Chief* .

Frampton, W. (2009, January). *Lincoln Police Hit With Layoffs*. Retrieved March 8, 2009, from News10.net: http://www.news10.net/news/local/story.aspx?storyid=53952

Goodman, M. D. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law and Technology* .

Griffith, D. (2003, November). *How to...Investigate Cybercrime: Tracking bad guys on the Net takes the experience of a detective and the know-how of a tech head.* Retrieved March 9, 2009, from POLICE Magazine: http://www.policemag.com/Articles/2003/11/How-to-Investigate-Cybercrime.aspx

Griffith, D. (2008, January). *The State of American Law Enforcement, Chapter 1: The Thinning Blue Line.* Retrieved March 8, 2009, from POLICE Magazine: http://www.policemag.com/Articles/2008/01/The-Thinning-Blue-Line.aspx

Griffiths, C. T., & al., e. (2006). *CIVILIANIZATION IN THE VANCOUVER POLICE DEPARTMENT.* Vancouver: Vancouver Police Department.

Hammond, R. (2003). Identity Theft: How to Portect Your Most Valuable Asset. In R. Hammond, *Identity Theft: How to Portect Your Most Valuable Asset* (pp. 64-69). New Jersey: Career Press.

http://www.internetworldstats.com. (2008, December 31). *INTERNET USAGE STATISTICS: The Internet Big Picture.* Retrieved March 8, 2009, from Internet World Stats: http://www.internetworldstats.com/stats.htm

Hudock, J. (2009, March). *How to Become a Detective.* Retrieved March 8, 2009, from Mahalo.com: http://www.mahalo.com/How_to_Become_a_Detective

Inside ID Theft. (2009, March 7). *Senior Citizen Identity Theft.* Retrieved March 7, 2009, from www.IdentityTheft.info: http://www.insideidtheft.info/seniors.aspx

Internet Crime Complaint Center. (2007). *2007 Internet Crime Report.* Retrieved March 8, 2009, from Internet Crime Complaint Center: http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf

Israelsen-Hartley, S. (2008, November 25). *Police Aim to Close Generation Gap.* Retrieved March 8, 2009, from LawOfficer.com: http://www.lawofficer.com/news-and-articles/news/utah_police_aim_to_close_generation_gap.html

Johnson, B. (2007, April 26). *The guardian.* Retrieved March 8, 2009, from guardian.co.uk: http://www.guardian.co.uk/technology/2007/apr/26/news.crime

Lagos, M. (2008, April 6). *SFPD lags behind in hiring civilians.* Retrieved March 8, 2009, from San Francisco Chronicle: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/04/05/BATQ1004MU.DTL

Legal-Criminal-Justice-Schools. (2009, March). *How to Become a Police Detective.* Retrieved March 8, 2009, from Legal-Criminal-Justice-Schools.com: http://www.legal-

criminal-justice-schools.com/Criminal-Justice-Degrees/How-to-Become-a-Police-Detective.html

McClatchy Newspapers. (2009, Febraury 22). *Rising crime could be recession's next effect.* Retrieved March 8, 2009, from Contra Costa Times: http://www.contracostatimes.com/ci_11759122

Palfrey, J., & Gasser, a. U. (2008). *Born Digital: Understanding the First Generation of Digital natives.* New York: Basic Books.

Powell, B. (2007, March 8). *Police struggle to keep up with savvy scammers.* Retrieved March 8, 2009, from TheStar.com: http://www.thestar.com/SpecialSections/article/188467

Purdue University. (2008, May 19). *Purdue to Assist FBI With Computer Crime: Press Release.* Retrieved March 8, 2009, from Inside INdiana Business: http://www.insideindianabusiness.com/newsitem.asp?id=29431

Sakal, M. (2009, February 28). *Mesa to use civilian investigators for less-serious crime.* Retrieved March 8, 2009, from East Valley Tribune : http://www.eastvalleytribune.com/story/136092

Schwartau, W. (2000). Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorsists, and Weapons of Mass Disruption. In W. Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorsists, and Weapons of Mass Disruption* (p. 368). New York: Thunder Mountain Press.

Scientific American. (2009, February). *Will the Recession Spark a Crime Wave?* Retrieved March 8, 2009, from Scientific American Inc: http://www.sciam.com/article.cfm?id=do-recessions-increase-crime

Scoville, D. (2008, May). *The State of American Law Enforcement, Chapter 5: Can the Average Cop Thrive in the Age of Specialization?* Retrieved March 9, 2009, from POLICE Magazine: http://www.policemag.com/Articles/2008/05/Can-the-Average-Cop-Thrive-in-the-Age-of-Specialization.aspx

U.S. Census Bureau. (2009, March 8). *Current Population Survey.* Retrieved March 8, 2009, from U.S. Census Bureau, Population Division: http://www.census.gov/main/www/popclock.html

Youngs, A. (2005). THE FUTURE OF INVESTIGATIONS. In A. e. Youngs, & J. A. Schafer (Ed.), *Policing 2020: Exploring the Future of Crime, Communities, and Policing* (pp. 208-211). Futures Working Group.